Goal of today: Solving a linear indefinite equation in the ring of polynomials by GB

Let K be a field. $K[x] = K[x_1, \ldots, x_n]$. We use the multi-index notation, e.g., $x^\alpha = \prod_{i=1}^n x_i^{\alpha_i}$. Let $w \in \mathbf{Z}^n$ be a vector, which we call a *weight vector*. We define a total order $<_w$ among monomials by

$$x^\alpha <_w x^\beta \quad \Leftrightarrow \quad \alpha \cdot w < \beta \cdot w$$
$$\text{or} \quad (\alpha \cdot w = \beta \cdot w \text{ and } \alpha <_{\mathrm{lex}} \beta)$$

where $\alpha <_{\mathrm{lex}} \beta$ when the first non-zero component of $\beta - \alpha$ is positive.

Example. $n = 2$, $w = (1, 1)$. (We use x, y instead of x_1, x_2.)

$$1 <_w y <_w x <_w y^2 <_w xy <_w x^2 <_w \cdots$$

$ax^\alpha <_w bx^\beta$, $a, b \in K$ is defined by $x^\alpha <_w x^\beta$ (ignore coefficients). In particular, $ax^\alpha =_w bx^\alpha$ (in the sense of order).

$$\mathrm{in}_{<_w}(f) = \text{ the leading term of } f \text{ by the order } <_w$$

Example.

$$\mathrm{in}_{<_w}(3xy + y^2 + 2x) = 3xy$$

For $f, g \in K[x]$, define $f <_w g$ iff $\mathrm{in}_{<_w}(f) < \mathrm{in}_{<_w}(g)$. Note that if $f <_w g$ then $hf <_w hg$ holds for any non-zero polynomial h.
f is called *divisible* by g with respect to $<_w$ when $\mathrm{in}_{<_w}(g) | \mathrm{in}_{<_w}(f)$.
Example. $\underline{3xy} + y^2 + 2x$ is divisible by $\underline{5x} + 1$.
Assume that a term m of f is divisible by g. Rewriting f to

$$f' := f - \frac{m}{\tilde{g}} g, \quad \tilde{g} = \mathrm{in}_{<_w}(g)$$

is called the *m-reduction* of f by g and denoted by

$$f \longrightarrow f' \quad \text{by } g$$

Example.

$$\underline{3xy} + y^2 + 2x \longrightarrow y^2 + \underline{2x} - \frac{3}{5}y \longrightarrow y^2 - \frac{3}{5}y - \frac{2}{5} \quad \text{by } 5x + 1$$

When $w_i > 0$ for $i = 1, \ldots, n$ m-reduction stops in finite steps, because there exists only finite lattice points α in the first orthant satisfying $\alpha \cdot w =$ (a given positive integer).
Exercise 1. Prove this fact when $w_i \geq 0$.
Let G be a finite set of polynomials. Assume that a term m of f is divisible by a polynomial g in G. (Add a figure of a monoideal.) We reduce f by g. The reduction, which is also called the m-reduction by G, is written as

$$f \longrightarrow f' \quad \text{by } G$$

If $w_i > 0$, the m-reduction by G stops in finite steps. When the m-reductions are performed as

$$f \longrightarrow f' \longrightarrow f'' \longrightarrow \cdots \longrightarrow \bar{f}$$

where $\bar{f}$ contains no divisible term by G. Then it is written as

$$f \longrightarrow^* \bar{f}$$

Example. $w = (1,1,1,1,1,1,1)$.
$t_1 >_w t_2 >_w y_1 >_w y_2 >_w y_3 >_w y_4$.

$$G = \{\underline{t_2} - y_1, \underline{t_3} - y_2, \underline{t_1 t_2} - y_3, \underline{t_1 t_3} - y_4\}$$

$$\begin{array}{lll} \underline{t_1 t_3} t_2 & \to & y_4 t_2 \quad \text{by } G \\ \underline{t_1 t_2} t_3 & \to & y_3 t_3 \to y_2 y_3 \quad \text{by } G \end{array}$$

When $f \to^* h$ by G, h is not necessarily unique.
Define

$$\mathrm{sp}(f,g) = \frac{\mathrm{lcm}(\tilde{f},\tilde{g})}{\tilde{f}} f - \frac{\mathrm{lcm}(\tilde{f},\tilde{g})}{\tilde{g}} g$$

where $\tilde{f} = \mathrm{in}_{<_w}(f) = ax^p$, $\tilde{g} = \mathrm{in}_{<_w}(g) = bx^q$,
$\mathrm{lcm}(\tilde{f},\tilde{g}) = \prod_{i=1}^n x_i^{\max(p_i,q_i)}$. (Add a figure of lcm.)

Theorem (Buchberger, 50 years ago)

Assume that $w_i \geq 0$. *We fix the order* $<_w$. *When the S-pair criterion*

$$\mathrm{sp}(g_i, g_j) \longrightarrow^* 0 \quad \textit{by } G$$

holds for any $g_i, g_j \in G$, $i \neq j$, *we have the following properties.*

1. (Standard representationi) *For any* $f \in \langle G \rangle$, *there exist* $h_i \in K[x]$ *such that*

$$f = \sum h_i g_i \quad \textit{and} \quad f \geq_w h_i g_i$$

2. (Ideal membership) *For* $f \in \langle G \rangle$ *we always have* $f \longrightarrow^* 0$ *by* G.
3. *If* $K[x] \ni f \longrightarrow^* u$ *by* G, *then* u *is unique, which is called the normal form of* f *by* G *and* $<_w$.

Example TGB.

$$G = \{\underline{t_2} - y_1, \underline{t_3} - y_2, \underline{t_1 y_1} - y_3, \underline{t_1 y_2} - y_4, \underline{y_1 y_4} - y_2 y_3\}$$

The set G satisfies the S-pair criterion.

$$t_1 t_2 t_3 \rightarrow t_1 t_3 y_1 \rightarrow t_1 y_1 y_2 \rightarrow y_2 y_3$$
$$t_1 t_2 t_3 \rightarrow t_1 t_2 y_2 \rightarrow t_2 y_4 \rightarrow y_1 y_4 \rightarrow y_2 y_3$$

Confluence of the m-reduction.

Proof

. Since $\mathrm{sp}(g_1, g_2) \to^* 0$ by G, we have

$$\mathrm{sp}(g_1, g_2) = c_1 g_1 - c_2 g_2 = \sum s_i g_i$$

where $c_1 g_1 =_w c_2 g_2 >_w s_i g_i$. Before proceeding to the proof, we introduce the important construction. We call the vector

$$(s_1 - c_1, s_2 + c_2, s_3, s_4, \ldots)$$

the syzygy vector of the S-pair $\mathrm{sp}(g_1, g_2)$ and denote it by $\mathrm{syzsp}(g_1, g_2)$. We have $\mathrm{syzsp}(g_i, g_j) \cdot G = 0$ where G is regarded as a vector $(g_1, g_2, \ldots)$.

Suppose that $f = \sum h_i g_i$. By changing indexes, we assume that

$$h_1 g_1 =_w h_2 g_2 =_w \cdots =_w h_k g_k >_w h_{k+1} g_{k+1} \geq_w \cdots$$

holds. If $k = 0$, then we have $f \geq_w h_i g_i$. We assume that $k > 0$. Since $\mathrm{in}_{<_w}(h_1 g_1) =_w \mathrm{in}_{<_w}(h_2 g_2)$, there exists $m = a x^\alpha$ such that $m \, \mathrm{in}_{<_w}(c_1 g_1) = \mathrm{in}_{<_w}(h_1 g_1)$.

Multiplying m to the syzygy of the S-pair $\mathrm{syzsp}(g_1, g_2)$ and adding it to the vector $(h_1, h_2, \ldots)$, we construct a new h' as

$$h' = (h_1 + s_1 m - c_1 m, h_2 + m(s_2 + c_2), h_3 + ms_3, h_4 + ms_4, \ldots).$$

Since $h'_1 g_1 <_w h_1 g_1$ and $h'_i g_i \leq_w h_i g_i$ for $i \geq 2$, k descreases or $\max_{<_w}(h'_i g_i)$ decreases for the new h'. Repeating this procedure, we obtain (1) in finite steps.

Conside the special case of $\sum h_i g_i = 0$. The important consequence of this proof is that the solution space of the linear indefinite equation (syzygy equation)

$$\mathrm{syz}(G) = \{h \in K[x] \mid \sum h_i g_i = 0\}$$

is generated by the syzygies of the S-pairs $\mathrm{syzsp}(g_i, g_j)$.
Exercise 2. Find the generators of the solutions of the linear indefinite equation for G in the Example TGB.